УДК 004.056

О ПРИМЕНЕНИИ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ В СИСТЕМАХ ПРЕВЕНТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Саламатова Т.А.,
научный руководитель канд. техн. наук, доцент кафедры безопасности информационных технологий Жуков В. Г.
Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева

Исследования в области обнаружения вторжений ведутся за рубежом больше четверти века. Исследуются признаки атак, разрабатываются и эксплуатируются методы и средства обнаружения попыток несанкционированного проникновения через системы защиты информации.

Для сертификации средств антивирусной защиты, средств обнаружения вторжений, систем предотвращения утечек данных и т.д. в схеме сертификации средств защиты информации ФСТЭК России существовал определенный порядок проведения испытаний — сертификация подобных продуктов до последнего времени проводилась на соответствие «Техническим условиям», что, по сути, означало полную недетерминированность процесса: поскольку требования к составу функциональных возможностей нигде не были формализованы, то под определение сертифицированного продукта одного и того же типа могли подпасть решения принципиально различных уровней.

Данная ситуация требовала пересмотра существующей нормативной базы в сфере сертификации средств защиты информации, поэтому для профессиональных участников рынка программного обеспечения в сфере информационной безопасности не стало неожиданностью принятие ФСТЭК требований к системам обнаружения вторжений (СОВ). Этот документ вступил в силу 15.03.2012 г. и имеет пометку «для служебного пользования», однако методические документы «Профили защиты» СОВ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, доступны на официальном сайте ФСТЭК России .

Под *системами обнаружения вторжений* (Intrusion Detection Systems, IDS) в документе понимаются программные и программно-аппаратные технические средства, реализующие функции автоматизированного обнаружения в информационных системах действий, направленных на преднамеренный несанкционированный доступ к информации, а также специальных воздействий на информацию в целях ее добывания, уничтожения, искажения или блокирования. СОВ рассматривается как один из базовых элементов системы защиты информационной системы, и в полном соответствии с общепринятой практикой в документе выделяются два типа систем обнаружения вторжений: системы обнаружения вторжений уровня сети (Network Intrusion Detection System , NIDS) и системы обнаружения вторжений уровня узла (Host-based Intrusion Detection System , HIDS)

Для каждого из вышеприведенных типов в требованиях к СОВ выделяются 6 классов защиты систем обнаружения вторжений в порядке ужесточения требований от шестого к первому.

В этих требованиях также указано то, что СОВ должны выполнять анализ собранных данных с целью обнаружения вторжений с использованием и сигнатурных методов, и эвристических методов одновременно.

Способ опознавания сигнатуры заключается в описании атаки в виде сигнатуры и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике, журнале регистрации и т.д.). В качестве сигнатуры атаки может выступать шаблон действий или

строка символов, характеризующие аномальную активность в автоматизированной системе.

Несмотря на эффективность сигнатурного метода, существует проблема создания такой сигнатуры, которая бы описывала все возможные модификации атаки. Для решения этой проблемы применяются эвристические методы. Данные методы помогает обнаруживать отклонения от нормального функционирования автоматизированной системы, используя эталонную модель функционирования. Вначале определяется типичные значения для таких параметров, как загруженность ЦПУ, активность работы диска, частота входа пользователей в систему и другие. Потом при возникновении значительных отклонений от этих значений система сигнализирует о возникшей ситуации.

На сегодняшний день насчитывается достаточно большое количество реализации СОВ, при этом, и в большинстве из них используется для анализа данных сигнатурный метод. Однако, согласно требованиям к методам анализа СОВ, представленных в нормативном документе ФСТЭК, алгоритмы анализа СОВ должны обладать свойствами, такими как адаптивность, самообучение, саморегуляция.

Перспективными для разработки алгоритмического обеспечения систем превентивной защиты информации, обладающими вышеназванными свойствами, являются методы, основанные на принципах работы нейронной сети, имитационного моделирования с использованием нечетких когнитивных карт, иммунной системы. Использование последнего метода в системах обнаружения вторжений (СОВ) является наиболее актуальным, так как сам принцип работы иммунной системы и свойства, которыми она характеризуется, максимально ориентированы на решение задачи обнаружения инцидентов информационной безопасности.

Искусственные иммунные сети (ИИС) строятся по аналогии с иммунной системой живого организма. Имеется достаточно много различий между живыми организмами и компьютерными системами, поэтому необходимы подобия, переносимые в компьютерную модель защиты. Искусственная иммунная система строится, как правило, только на двух центральных положениях: антиген – антитело.

В качестве антигенов выступают системные вызовы или сетевые пакеты. При первичной встрече иммунной системы с антигеном — он изучается, и на основании составленного шаблона вырабатываются антитела: уничтожающие, блокирующие или пропускающие антиген.

В настоящее время существует несколько вычислительных моделей, основанных на принципах работы иммунной систем. Одним из вариантов искусственной иммунной системы является модель иммунной сети Ерне. Н.К. Ерне предложил гипотезу, согласно которой иммунная система представляет собой регулируемую сеть молекул и клеток, распознающих друг друга даже при отсутствии антигена. Такие структуры часто называют идиотипическим сетями, они служат математической основой для изучения поведения иммунной системы.

Другим вариантом создания системы, основанной на принципах работы иммунной системы человека, является алгоритм отрицательного отбора. Профессор университета Нью-Мексико С. Форрест предложил алгоритм отрицательного отбора для обнаружения изменений, построенный на основе принципов распознавания своего и чужого в системе иммунитета.

Теория клональной селекции используется с тем, чтобы объяснить, как иммунная система “борется” против чужеродных антигенов. Когда антиген проникает в наш организм, она начинает размножаться и поражать своими токсинами клетки нашего организма. Те клетки, которые способны распознавать чужеродный антиген, размножаются способом, пропорционально степени их распознавания: чем лучше распознавание антигена, тем большее количество потомства (клонов) было сгенерировано. В течение

процесса репродукции клетки отдельные клетки подвергаются мутации, которая позволяет им иметь более высокое соответствие (аффинность) к распознаваемому антигену. Обучение в иммунной системе обеспечивается увеличением относительного размера популяции и аффинности тех лимфоцитов, которые доказали свою ценность при распознавании представленного антигена. Основными иммунными механизмами при разработке алгоритма являются обработка определенного множества антител из набора клеток памяти, удаление антител с низкой аффинностью, созревание аффинности и повторный отбор клонов пропорционально их аффинности к антигенам.

Схема ИИС на основе модифицированного алгоритма клональной селекции представлена на рисунке 1. Основным отличием данной реализации алгоритма от классической является процедура мутации.

В ИИС детекторы и антигены имеют формальное представление в виде множеств над конечным алфавитом. Без потери общности допустим, что мощность множеств детекторов D и антигенов A одинаковая и задана статично. В таком случае под *аффинностью* антигенов с детекторами понимается частичное соответствие элемента $a_i \in A$ элементу $d_i \in D$. Аффинность растет с увеличением количества идентичных элементов.

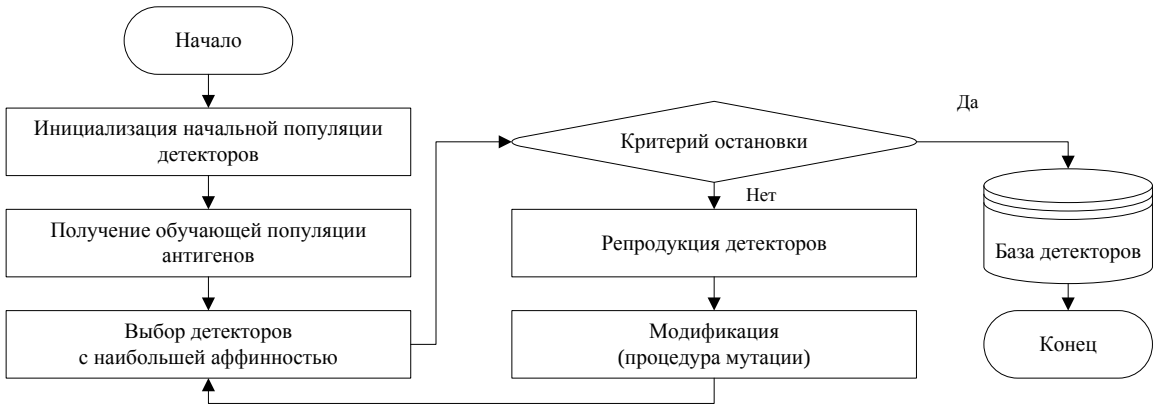

Рисунок 1 — Модифицированный алгоритм клональной селекции

Обучающей выборкой называется такой набор $(\alpha_1, \beta_{1j}), (\alpha_2, \beta_{2j}), \dots (\alpha_i, \beta_{ij})$, для которых $i \in [0,19]$, $j \in [0,2]$. Выбор $j = 3$ для α_i обусловлен проведенными исследованиями, в ходе которых j изменялось в диапазоне от 2 до 19.

Аффинность антигена α_i к детектору β_{ij} рассчитывалась как $\sum_{x=1}^{m} \begin{cases} 1, if\ \alpha[x] = \beta_{ij}[x] \\ 0, \text{else.} \end{cases}$, где m — мощность множества α_i .Согласно рассчитанной аффинности происходит упорядочивание детекторов по убыванию. Затем осуществляется репродукция первых k детекторов с последующей перезаписью детекторов с низкой аффинностью. Количество наследников (клонов) каждого детектора равняется количеству антигенов заданной обучающей выборки.

Модификация детектора осуществляется путем замены n элементов на элементы из конечного алфавита. Выбор элемента из конечного алфавита осуществляется с помощью генератора псевдослучайных чисел на основе алгоритма Блюма-Блюма-Шуба (Blum - Blum - Shub, BBS). Критерием остановки считается достижение 20%-ого порога аффинности детектора к каждому антигену.

Для исследования эффективности модифицированный алгоритм клональной селекции был реализован программно. Программа для ЭВМ состоит из двух модулей: Genereto r и Analizator.

Модуль Genereter создает обучающую выборку и записывает их для последующего анализа в базу данных (БД) антигенов. На основе сформированной БД антигенов с помощью модифицированного алгоритма клональной селекции вырабатываются детекторы, которые, в свою очередь, заносятся в БД детекторов.

Модуль Analizator получает на вход антигены из БД антигенов и детекторы из БД детекторов. Входные антигены α_i подвергаются модификациям с разным количеством изменяемых элементов (период изменения $T = \overline{1,9}$). Модифицированные антигены α_i' обрабатываются алгоритмом поиска детекторов. Данный алгоритм осуществляет поиск детектора β_{ij} на этот антиген α_i' в БД детекторов. Для исследования эффективности алгоритма, были сгенерированы тестовые данные, с параметрами: алфавит $M = \overline{0,9}$, размер α_i — 80 символов, размер частичного соответствия: 20% от размера α_i. Результаты исследования приведены в таблице 1, рисунке 2.

Таблица 1 — Результаты исследования эффективности алгоритма при k=3

α_i	β_{ij}	**Количество обнаруженных изменений при заданном периоде изменения, T**								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
40	6	40	35	34	29	30	26	19	24	23
120	18	119	107	103	83	79	76	77	64	61
200	30	199	173	184	144	138	135	133	120	106
280	42	263	257	224	181	169	159	155	131	144
360	54	356	328	270	271	219	228	186	206	182
440	66	380	388	315	309	254	261	212	243	194
520	78	493	445	399	355	300	314	276	253	236

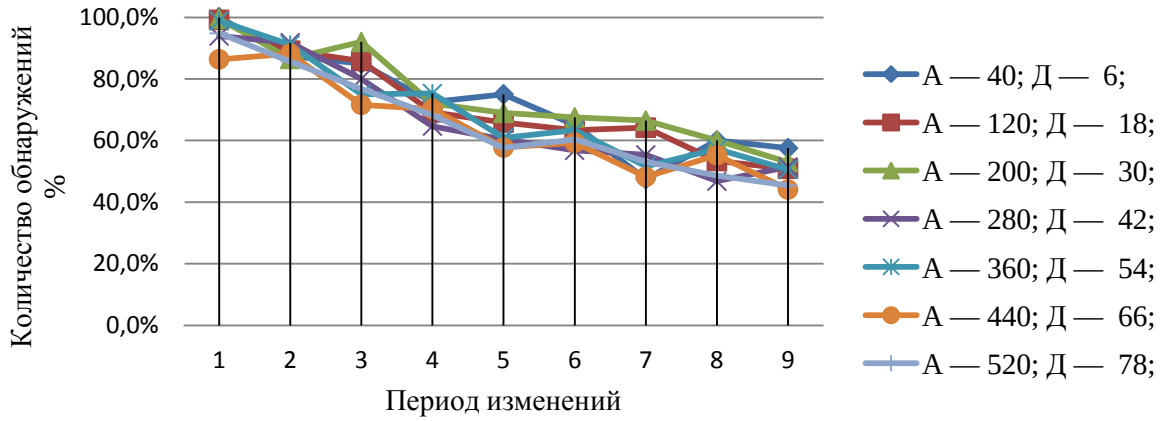

Рисунок 2 — Результаты тестирования модифицированного алгоритма клональной селекции. График зависимости количества обнаруженных изменений от внесенных изменений

На представленном графике (рисунок 2) видно, что с уменьшением количества внесенных изменений процент обнаружения изменений в исследуемом множестве падает. Объясняется это тем, что внесенные изменения попали в неконтролируемый участок данных детектора β_{ij}. При создании детектора β_{ij} невозможно предугадать, какие участки входящих данных будут контролироваться, и это в свою очередь затрудняет внесение изменений и внедрения вредоносных данных.

Результаты проведенных исследований показывают, что ИИС с клональной селекцией позволяют обнаружить преднамеренные изменения в контролируемых данных. Таким образом, применение ИИС в качестве эвристических методов анализа систем превентивной защиты информации позволит эффективно решать задачи выявления аномалий в действиях пользователя ИС и сетевого трафика.